

UNITED STATES DISTRICT COURT

FILED

JUN 29 2022

for the
Northern District of Oklahoma

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of
Information Associated with Apple ID
TONIESPARZA25@ICLOUD.COM that is Stored at a
Premises Controlled by Apple Inc.

)
)
) Case No. 22-MJ-406-JFJ
)
) **FILED UNDER SEAL**
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *Information Associated with Apple ID TONIESPARZA25@ICLOUD.COM that is Stored at a Premises Controlled by Apple Inc.:*

See Attachment "A"

located in the Northern District of California, there is now concealed *Information Associated with Apple ID TONIESPARZA25@ICLOUD.COM that is Stored at a Premises Controlled by Apple Inc.:*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

21 U.S.C. § 846

Conspiracy to Distribute Controlled Substances

The application is based on these facts:

See Affidavit of SA Taylor Wilson, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

T. Wilson

Applicant's signature

Taylor Wilson, Special Agent, DEA

Printed name and title

Sworn to before me by phone.

Date: 6/29/22

City and state: Tulsa, Oklahoma

Jodi Jayne

Judge's signature

Susan E. Huntsman, U.S. Magistrate Judge

Printed name and title

Jodi Jayne

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Information Associated with Apple ID
TONIESPARZA25@ICLOUD.COM
that is Stored at a Premises Controlled
by Apple Inc.**

Case No. _____

FILED UNDER SEAL

Affidavit in Support of an Application for a Search Warrant

I, Special Agent Taylor Wilson, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at a premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, in Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government information (including the content of communications) in its possession associated with the Apple ID TONIESPARZA25@ICLOUD.COM, as further described in Section I of Attachment B. Upon receipt of the information described in Section I of

Attachment B, government-authorized persons will review the information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I am a Special Agent with the Drug Enforcement Administration (DEA), United States Department of Justice (DOJ). I have been a DEA Special Agent since March 2016. I am currently assigned to the Tulsa Resident Office (TRO), in Tulsa, Oklahoma, and I am an "investigative or law enforcement officer" of the United States as defined in 21 U.S.C. § 878(a). I was previously employed with Customs and Border Protection (CBP), Department of Homeland Security. I worked as a CBP Officer for approximately two years.

4. During my law enforcement career, I have received countless hours in specialized training from various federal law enforcement agencies. This training has focused upon methods of unlawful manufacturing of illegal narcotics via clandestine laboratories, the installation and monitoring of global positioning satellite (GPS) trackers, Title III wire interceptions, smuggling and distribution techniques, methods of drug trafficking, as well as the means by which drug traffickers derive, launder and conceal their profits from drug trafficking, the use of assets to facilitate unlawful drug trafficking activity and the law permitting the forfeiture to the United States of assets purchased with drug proceeds or assets used or intended to be used to facilitate the

drug violations. I have gained a considerable amount of knowledge about drug trafficking organizations and their members through my training and experience. During the course of my training and interviews with various defendants I have learned how individuals involved in drug distribution schemes maintain records and conspire to deceive law enforcement as well as rival distributors of controlled dangerous substances. I have learned how individuals who are involved in the distribution of controlled dangerous substances maintain records and secret monies derived from the sale of illegal drugs.

5. Based on my experience as a law enforcement officer, I also know that those involved in international drug trafficking rely heavily on telephones to communicate with one another in order to coordinate the smuggling, transportation, and distribution of illegal drugs, and that they frequently employ coded language and slang terminology in an effort to maintain secrecy while engaging in such communications.

6. Through my employment as a law enforcement officer, I have gained knowledge in the use of various investigative techniques, including the use of wire and electronic interceptions and other types of electronic surveillance, physical surveillance, undercover investigators, confidential informants, cooperating witnesses, controlled purchases of illegal drugs, consensually-monitored recordings, investigative interviews, trash searches, mail covers, financial investigations, administrative and grand jury subpoenas, and search and arrest warrants.

7. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

8. Based on my training, research, experience, and the facts as set forth in this affidavit, there is probable cause to believe the identified Apple ID contains evidence of violations of 21 U.S.C. § 846, conspiracy to distribute controlled substances by FNU LNU (a/k/a UM1954).

Jurisdiction

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

10. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Apple Inc. from notifying the

subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Probable Cause

11. In approximately January 2020, members of the Drug Enforcement Administration (DEA) Tulsa Resident Office (TRO), the Tulsa Police Department (TPD), and the DEA Oklahoma City District Office (OCDO) began investigating a drug trafficking organization (DTO) distributing cocaine in Tulsa, Oklahoma, and other parts of the United States. During this investigation, investigators identified FNU LNU (a/k/a “Chuy”) to be a Mexico-based cocaine source of supply (SOS).

12. On August 13, 2021, the Honorable Timothy DeGiusti, Chief Judge for the Western District of Oklahoma (WDOK), signed an order authorizing the interception of wire and electronic communications on telephone number (405) 625-9026, which is known to be used by Maria Julia Baeza-Medrano (Baeza-Medrano).

13. On August 18, 2021, DEA OCDO investigators intercepted a series of calls between Aaron Baeza-Medrano (Aaron), using Baeza-Medrano’s telephone, and telephone number (918) 361-1954, which is known to be used by FNU LNU (a/k/a UM1954). During these calls, UM1954 and Aaron discussed Aaron delivering an unknown quantity of cocaine from Oklahoma City to UM1954 in Tulsa. UM1954 advised Aaron that the cocaine was not his and the ultimate recipient of the cocaine had arrived to Tulsa from out of town. Additionally, Aaron and UM1954 discussed the quality of the cocaine. Aaron stated, “these are clean,” and UM1954 advised,

“the guys are going to check that work, cousin.” Moreover, UM1954 and Aaron agreed to meet at O'Reilly Auto Parts, located near 31st and Garnett in Tulsa. Following the meeting, investigators observed UM1954 and Aaron travel into the neighborhood to the north. However, investigators ultimately lost physical surveillance of UM1954 and Aaron and surveillance was terminated.

14. In September 2021, members of the DEA TRO and the TPD began investigating the drug trafficking activities of Christian Ramirez. Investigators have identified Ramirez to use telephone number 918-693-0190 and to sell cocaine and methamphetamine from his residence, located at 236 South 120th East Avenue, Tulsa, Oklahoma.

15. During this investigation, investigators have determined that the service provider for 918-361-1954 is Sprint/T-Mobile. Additionally, investigators have identified telephone number 918-361-1954 to be subscribed to Guadalupe Mosqueda at 3814 South 82nd East Avenue, Tulsa, Oklahoma. During this investigation, investigators have identified UM1954 to reside at 2915 South 106th East Avenue, Tulsa, Oklahoma. Additionally, investigators have identified telephone number 918-361-1954 to have a WhatsApp account associated its telephone number 918-361-1954.

16. On April 29, 2022, United States Magistrate Judge Jodi F. Jayne, Northern District of Oklahoma, signed an order authorizing the installation and use of pen registers and trap and trace devices for the WhatsApp account associated with telephone number 918-361-1954. Investigators have used the data obtained from the

pen register and trap and trace device for the WhatsApp account associated with telephone number 918-361-1954 to identify the device for telephone number 918-361-1954 is an iPhone. For example, when UM1954 sends an outgoing message on WhatsApp, the pen register and trap and trace device shows, "From: 19183611954 Device: iphone."

17. Based on my training and experience, I know iPhones to use iCloud to store data from the respective telephone. In this situation, I believe the iCloud account associated with telephone number 918-361-1954 will provide information showing UM1954's involvement with the trafficking of cocaine in the Northern District of Oklahoma. Additionally, I believe the iCloud account associated with telephone number 918-361-1954 will assist investigators with identifying other known and unknown co-conspirators within this DTO.

18. On June 2, 2022, United States Magistrate Judge Jodi F. Jayne, Northern District of Oklahoma, signed a 2703(d) order authorizing investigators to receive the iCloud account associated with telephone number 918-361-1954. Subsequently, Intelligence Analyst (IA) Ruth Aston served the 2703(d) order to Apple via email.

19. On June 10, 2022, Apple responded to the 2703(d) and provided IA Aston with a link to download the response to the 2703(d) order requesting the iCloud account associated with telephone number 918-361-1954.

20. On June 21, 2022, Tulsa Police Department (TPD) Officer Booth extracted the information from Apple. On this same date, your affiant and TFO Drew Sharp

identified iCloud account toniesparza25@icloud.com to be associated with telephone number 918-361-1954.

21. On June 28, 2022, DEA TRO investigators conducted toll analysis of telephone numbers in contact with UM1954 at telephone number 918-361-1954. Investigators identified telephone number 918-361-1954 to be in contact with Ramirez, with the last contact on May 5, 2022. Additionally, DEA TRO investigators conducted toll analysis of telephone numbers in contact with UM1954 via WhatsApp on 918-361-1954. Investigators identified telephone number 918-361-1954 to be in contact with telephone number 918-927-2927, with the last contact on June 25, 2022. Investigators know telephone number 918-927-2927 to be used by Manuel Esparza-Escobedo. Additionally, investigators have identified Esparza-Escobedo to be in communication with Manuel Salacies Jr. and Ariana Delgado. During this investigation, investigators have identified Salacies and Delgado to be Mexico-based members of the "Chuy" DTO.

Background Concerning Apple¹

22. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

23. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). The services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names including, but not limited to mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

f. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

24. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

25. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The

subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

26. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

27. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the

telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

28. Apple provides users with approximately five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also

be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

29. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

30. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

31. Based on my training and experience, I know law enforcement can often retrieve messages and data deleted on Apple iPhones from iCloud back-ups. Further, stored communications and files connected to the targeted accounts may provide direct evidence of the offenses under investigation. In addition to the actual content of said communications, the user's account activity, date-time logs, geo-location data, and other information retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is critical because it allows

investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation, and is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Alternatively, this same information may help to exclude the innocent from further suspicion.

32. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under

investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

34. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

Information to be Searched and Things to be Seized

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information

described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

37. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

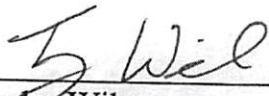
Conclusion

38. Based on the information above, I submit that there is probable cause to believe that there is evidence of violations of title 21 U.S.C. § 846, conspiracy to

distribute controlled substances associated with the Apple ID described in Attachment A.

39. I request to be allowed to share this affidavit and the information obtained from this search (to include copies of digital media) with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,



Taylor Wilson
Special Agent
Drug Enforcement Administration

Subscribed and sworn by phone on June 29th, 2022.



SUSAN E. HUNTSMAN *Jodi Jayne*
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the Apple ID toniesparza25@icloud.com that is stored at a premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California, 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media

Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from August 1, 2021, through and including June 21, 2022, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from August 1, 2021, through and including June 21, 2022, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud account from August 1, 2021, through and including June 21, 2022, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers) account from August 1, 2021, through and including June 21, 2022, including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations account from August 1, 2021, through and including June 21, 2022 where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken between August 1, 2021, through and including June 21, 2022; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

1. All information described above in Section I that constitutes evidence of violations of 21 U.S.C. § 846, conspiracy to distribute controlled substances including, for each account or identifier listed on Attachment A:

- a. The sale of illegal drugs;
- b. Evidence indicating other accounts used by the owner of the Apple ID;
- c. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- d. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and the account subscriber;

e. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

f. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

g. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.